Special Supplement to ***Dateline DHMH***

What is HIPAA?

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress and signed by President Clinton. The portion of this law which provides important federal protections for the continuation of health insurance benefits when an employee changes health plans, accepts a new job, or experiences a layoff is already in effect. HIPAA regulations governing administrative simplification will be implemented over the next few years.

Administrative simplification

HIPAA will address the administrative costs of healthcare delivery by establishing uniform data standards; facilitating electronic transmission of information throughout the industry; and combating insurance and provider fraud and abuse.

Regulations implementing HIPAA will require extensive changes to virtually all computerized healthcare systems that incorporate data for medical transactions, diagnostic and procedure codes, identifiers, and electronic medical records.

HIPAA privacy and security

HIPAA requires agencies to provide the privacy and security necessary to protect electronic health data. The requirements are expected to alter the business practices of every healthcare entity. These safeguards establish basic protections for the integrity, security, and privacy of every U.S. citizen's health information.

All medical records and other individually "identifiable" health information, whether in electronic, written, or verbal format, are protected by the HIPAA privacy regulations. While HIPAA privacy regulations will cause dramatic change in other states, in Maryland most of HIPAA's provisions are similar to ones already in place under Maryland law.

Disclosure of individually "identifiable" health information

With few exceptions or explicit authorization from an individual, health information may only be used for purposes related to health care. Disclosure of this information will be limited to the minimum necessary to accomplish the stated purpose. There are exceptions, when disclosures are permitted without explicit permission, but these are limited and clearly defined.

Compliance and penalties

Compliance for electronic transactions by large health care entities like DHMH is required by October 16, 2002 and privacy compliance is required by April 14, 2003. The final rules for other HIPAA requirements are still pending.

The penalties for non-compliance with any of the HIPAA electronic transaction provisions are cumulative civil fines. Intentional breaches of privacy can subject organizations and individuals to civil and criminal penalties.

Continued on next page

HIPAA IMPACTS YOUR JOB AS A DHMH EMPLOYEE

DHMH compliance

HIPAA affects all of DHMH and will require changes to business processes and procedures, operations, and information technology. Each DHMH business unit is responsible for reaching HIPAA compliance. As with Y2K, the Information Resources Management Administration is coordinating this process with assistance from the HIPAA Workgroup established by the DHMH Health Information Coordinating Council.

HIPAA workgroup and subworkgroups

The HIPAA Workgroup is chaired by Joe Davis, Executive Director, Operations and Eligibility Medical Care Programs (Medicaid), and is divided into five subworkgroups:

1) Due Diligence Documentation and Legal Agreements;
2) Transactions;
3) Code Sets and Identifiers;
4) Security and Privacy; and
5) Education, Training and Awareness.

Each subworkgroup member will be proficient with the information and details of the federal HIPAA regulations in his or her assigned area. The groups will also collaborate, facilitate,

Continued on next page

Summary of Responsibilities by Job Function

Job Function	*Privacy*	*Security*	*Transaction Code Sets Identifiers*	*Legal Agreements*	*Due Diligence*
All Employees	X	X			
Custodian of Records	X	X	X	X	X
Data Stewards	X	X	X	X	X
Designated Responsible Parties	X	X	X	X	X
IRB/Privacy Board Members	X	X	X	X	X
System Administrators	X	X	X	X	X
Data Technicians	X	X	X		
Contract Preparers	X	X		X	X
Contract Monitors	X	X	X	X	X
Staff Handling Medical Records	X	X		X	X
Staff Conducting Medical Billing	X	X	X	X	
Volunteers	X	X			

HIPAA Liaisons	Limit liability by ensuring HIPAA compliance for specified business unit, and maintaining the required "due diligence" documentation.
Patients, Guardians, and Families	Provide education on Patient Rights, including informed consent. Provide written policies for the disclosure of information.
Business Associates and Other Disclosurers	Provide awareness of necessary changes required by HIPAA. Provide written policies/procedures to reduce DHMH's exposure to liability. Establish Chain-of-Trust Agreements. Monitor compliance, as necessary, to limit DHMH liability.
Vendors	Provide awareness of necessary changes required by HIPAA. Incorporate necessary legal language in to RFPs, contracts, and MOUs. Monitor compliance.

and provide general monitoring of HIPAA compliance (without conducting, policing, or certifying the actual compliance) to all units within the DHMH organizational structure.

Since HIPAA is not just a one-time issue, ongoing DHMH enforcement/compliance procedures are also in development.

DHMH electronic healthcare transactions

HIPAA standardizes a variety of electronic transactions currently used for paying claims for the health services provided to recipients.

All DHMH systems used for processing electronic transactions must become HIPAA-compliant for transactions, code sets, and identifiers.

Anyone entering, reviewing, analyzing or transmitting transaction data will be impacted by these federal standards.

DHMH privacy and security

HIPAA requires agencies to establish privacy and security policies and procedures to protect individually "identifiable" information. The privacy rules limit disclosures of health information. This also means staff must not inappropriately discuss health information.

For electronic security, the computer networking staff will implement most of the required measures.

All DHMH employees are expected to know and understand the DHMH privacy and security policies and unit procedures. Under these procedures, employees should not share their computer passwords and should limit physical access to medical records and other protected information.

DHMH legal agreements

HIPAA requires new legal language and/or documents to be established and monitored as necessary to limit liability. The groups affected by these requirements are business partners, outside entities authorized to receive information, and vendors.

Many of the necessary documents are already in development/review by the DHMH Office of the Attorney General. Examples include:
1) warranty of liability language to ensure vendors deliver HIPAA compliant products;
2) new provisions for contracts;
3) new provisions for MOUs (memorandums of understanding); and
4) a standard format for Chain-of-Trust Agreements.

Patients must be informed of their rights and the agency privacy practices. In addition,

Continued on next page

KEYS TO COMPLIANCE

The key to **transaction compliance** is: Don't panic; once the electronic transaction systems are changed and tested, each business unit will provide system specific training.

If it is necessary for you to disclose health data, the key to **privacy compliance** is: You must understand State and federal privacy laws. Also, remember to treat all health information the way you want others to treat your information.

The key to **security compliance** is: When in doubt, ask your supervisor, your security officer, or your privacy officer.

When dealing with **legal documents or issues**, the key to compliance is: If you are responsible for legal agreements, work with your AG and your procurement officer to ensure you understand the documents and how to implement/monitor compliance.

If you are a **HIPAA Liaison**, the key to compliance is: Limit DHMH and business unit liability by monitoring internal compliance and maintaining the required "due diligence" documentation.

they will be asked to sign consent or authorization forms. Current consent forms are being revised in light of HIPAA.

DHMH due diligence

Limiting liability for HIPAA compliance requires proof of "due diligence" (i.e., making required and reasonable efforts to reach compliance). This is the responsibility of the HIPAA Liaison for each business unit (e.g., an administration, a local health department, or a facility). To assist with these efforts, the HIPAA subworkgroups are developing guidelines, check lists, and other compliance implementation tools.

HIPAA IMPACTS YOU PERSONALLY AS A HEALTH CARE CONSUMER

Although you will not see the electronic transactions, over time you will benefit from HIPAA through reduced paperwork, fewer hassles, and lower transaction costs.

The use of the standard HIPAA transactions will rapidly become routine practice. The process may start with the electronic transfer of your eligibility and premium payment information from your employer to the health insurer you select.

When you go to a doctor or other health care provider, their office will be able to verify your eligibility/coverage and handle any necessary referrals/pre-authorizations. They will also be able to submit the claim for payment, check the status of the claim, and provide additional information to process the claim. Also, if you have multiple health plans, the claim can be forwarded from one payer to the next. All of this can occur electronically.

Your medical records and other identifiable health information are subject to HIPAA protections for privacy and security. When combined with the Maryland Confidentiality of Medical Records Act already in effect, your rights as a consumer will ensure that:

- Your doctor, other providers, and health plans provide you with a clear written explanation of how they may use and disclose your health information.
- You will be able to see and get copies of your records, and request amendments.
- You will be able to obtain a history of non-routine disclosures.
- Your doctor and other health care providers will obtain your consent before sharing your information for treatment, payment, and health care operations.
- You will be asked to sign a separate authorization form for disclosures not related to health care.
- You will have the right to restrict the uses and disclosures of your information.

If your privacy protections are violated (those provided by HIPAA or by the policies or procedures of the covered entity), you will have the right to file a formal complaint with the provider, the health plan, or the federal Department of Health and Human Services Office of Civil Rights. You may also have access to the courts under Maryland law.

Conclusion

HIPAA is said to be the first step toward making healthcare an e-business. In the future, you will be able to electronically authorize your various health care providers to exchange portions of your computerized medical record. This will improve the coordination, effectiveness, and efficiency of your care.

Remember that 30 years ago, no one expected to walk up to a machine in a wall, insert a plastic card, and receive money from their checking/savings account. ATMs have changed the way we bank, and HIPAA will change the way healthcare is administered.

For more HIPAA information

The DHMH website has a special section that contains more information on HIPAA. The Internet address is *www.dhmh.state.md.us/HIPAA.* The links to the fact sheets may be especially useful.